原始多項式ではない既約多項式で構成する $GF(2^4)$

情報数理学特別講義I 第3回補足

2025-11-05

ゴール

- $GF(2)$ 上4次の既約だが原始ではない多項式 $f(x)$ を用いて $GF(2^4)$ を構成する.
- $f(x)$ の根 α が $2^4 - 1 = 15$ を生成せず，15 より小さな位数で 1 に戻ることを式で示す.
- 原始多項式を使わないと何が起こるかを感覚的に理解する.

$GF(2^4)$ を構成する既約多項式

- $f(x) = x^4 + x^3 + x^2 + x + 1$.
- $f(0) = 1$, $f(1) = 1$ より 1次因子を持たない.
- 2次の既約多項式 $x^2 + x + 1$ でも割り切れないので $f(x)$ は既約である.

$GF(2^4)$ の構成

- $GF(2)[x]/(f(x))$ を $GF(2^4)$ とみなし，$\alpha = [x]$ を $f(\alpha) = 0$ を満たす代表とする.
- 各元は $a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3$ で表現し，加算は係数ごとに $GF(2)$ の和を取る.
- 乗算は $\alpha^4 = x^4 \equiv x^3 + x^2 + x + 1$ を用いて次数4以上を繰り下げる.

αの冪を計算して位数を確かめる

$$
\begin{aligned}
\alpha^4 &= \alpha^3 + \alpha^2 + \alpha + 1 \\
\alpha^5 &= \alpha(\alpha^4) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = 1 \\
\alpha^6 &= \alpha, \quad \alpha^7 = \alpha^2, \quad \alpha^8 = \alpha^3
\end{aligned}
$$

- α の位数が5なので，原始元にはならない．

この体上での原始元とべき表現と多項式表現

- この体でも位数15の元γが存在し，$\gamma = \alpha + 1$と定義する.
- 任意の非零元aは唯一の$0 \leq k \leq 14$で$a = \gamma^k$と書ける.
- 下表は原始元γの冪と多項式表現，および基底$(1, \alpha, \alpha^2, \alpha^3)$に対する係数ベクトルの対応.

k	γ^k (多項式)	ベクトル表現	k	γ^k (多項式)	ベクトル表現
0	1	$(1,0,0,0)$	8	$1+\alpha^3$	$(1,0,0,1)$
1	$1+\alpha$	$(1,1,0,0)$	9	α^2	$(0,0,1,0)$
2	$1+\alpha^2$	$(1,0,1,0)$	10	$\alpha^2+\alpha^3$	$(0,0,1,1)$
3	$1+\alpha+\alpha^2+\alpha^3$	$(1,1,1,1)$	11	$1+\alpha+\alpha^3$	$(1,1,0,1)$
4	$\alpha+\alpha^2+\alpha^3$	$(0,1,1,1)$	12	α	$(0,1,0,0)$
5	$1+\alpha^2+\alpha^3$	$(1,0,1,1)$	13	$\alpha+\alpha^2$	$(0,1,1,0)$
6	α^3	$(0,0,0,1)$	14	$\alpha+\alpha^3$	$(0,1,0,1)$
7	$1+\alpha+\alpha^2$	$(1,1,1,0)$	15	1	$(1,0,0,0)$